UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,203	12/04/2003	Wajdi K. Feghali	42P14932	2146

8791 7590 01/19/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	**PAPER NUMBER**
2112	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/730,203	FEGHALI, WAJDI K.	
	Examiner	Art Unit	
	Oscar A. Louie	2112	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/04/2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the original filing of 12/04/2003. Claims 1-41 are pending and have been considered as follows.

Examiner's Note

1. The Applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in Claim 35 by using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer program modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Claim Objections

2. Claim 16 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 16 discloses, "The machine-readable medium of claim 16 where in the method," however, it is noted by the examiner that this will be interpreted as Claim 16 is dependent on Claim 15 instead of itself.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 17, 23, & 28 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 17, 23, & 28 all use the term "dependencies" without further disclosing the explicit definition or details of these dependencies. It is very difficult to determine exactly what "dependencies" refers to. It is noted by the examiner that these "dependencies" will be interpreted as referring to any aspects of the invention that have direction correlation to the conditions of the invention that may cause an unwanted amount of efficiency degradation in the system, method, or apparatus that is claimed by the applicant.

5. Claims 25 & 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite in that it fails to point out what is included or excluded by the claim language. This claim is an omnibus type claim. The terms "substantially" and "approximately" in Claims 25 & 26 respectively are omnibus and relative terms. They do not distinctly clarify the scope of the invention due to the nature of their definitions. It is recommended by the examiner that the applicant specify a more precise measurement of acceptable frequencies as disclosed and applicable to the invention in Claims 25 & 26.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-13, 15-24, & 27-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Kaufman (US-5491752-A).

Claim 1:

Kaufman discloses a processor comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "a plurality of pipeline stages to perform an inner loop of a hash algorithm, the plurality of pipeline stages comprising at least as many pipeline stages as there are iterations of the inner loop to be performed") [column 1 lines 20-31].

Claim 2:

Kaufman discloses a processor as in Claim 1 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "the plurality of pipeline stages further comprises as many pipeline stages as there are chaining variables to be used in the inner loop") [column 1 lines 20-31].

Claim 3:

Kaufman discloses a processor as in Claim 2 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication

tokens" (i.e. "each pipeline stage comprises an adder, a shifter, and logic to perform a function") [column 1 lines 20-31].

Claim 4:

Kaufman discloses a processor as in Claim 3 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "control logic to schedule operations to be executed within the plurality of pipeline stages") [column 1 lines 20-31].

Claim 5:

Kaufman discloses a processor as in Claim 4 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a

related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "operations are to be scheduled by the control logic and executed by the plurality of pipeline stages so as to minimize data dependencies between iterations of the inner loop to be performed") [column 1 lines 20-31].

Claim 6:

Kaufman discloses a processor as in Claim 5 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the hash algorithm is chosen from a group of secure hash algorithms

(SHA) consisting of SHA-1, SHA-128, SHA-196, SHA-256, and message digest 5 (MD5)") [column 9 lines 41-60].

Claim 7:

Kaufman discloses a processor as in Claim 6 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the hash algorithm is to be performed at an operating frequency equal to that of the adder") [column 9 lines 41-60].

Claim 8:

Kaufman discloses a processor as in Claim 7 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "the plurality of pipeline stages comprises 88 pipeline stages to process 512 bits of data") [column 1 lines 20-31].

Claim 9:

Kaufman discloses an apparatus comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data

item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "a first plurality of pipeline stages to perform a hash including: a first pipeline stage to add a first constant to a first data word to yield a first result; a second pipeline stage to add the first result a first chaining variable, perform a first function on a second, third, and fourth chaining variable to yield a second result, and add the first constant to a second data word to yield a third result; a third pipeline stage to add the second result to the sum of a fifth chaining variable and the first result, add the first constant to a third data word, add the third result to the fourth chaining variable, perform the first function on the first, second, and third chaining variables after they each of have been shifted by a plurality of bits; a second plurality of pipeline stages to add an initial state of the first, second, third, fourth, and fifth chaining variables to a final state of the first, second, third, fourth, and fifth chaining variables, respectively") [column 9 lines 41-60].

Claim 10:

Kaufman discloses an apparatus as in Claim 9 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing

algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the first plurality of pipeline stages comprises 83 pipeline stages to process 512 bits of information") [column 9 lines 41-60].

Claim 11:

Kaufman discloses an apparatus as in Claim 9 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-

way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the second plurality of pipeline stages comprises 5 pipeline stages to process 512 bits of information") [column 9 lines 41-60].

Claim 12:

Kaufman discloses an apparatus as in Claim 9 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed

on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the first and second plurality of pipeline stages are implemented within a network processor architecture") [column 9 lines 41-60].

Claim 13:

Kaufman discloses an apparatus as in Claim 9 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash

Algorithm)" (i.e. "the hash algorithm is a secure hash algorithm (SHA) and the plurality bits is 30") [column 9 lines 41-60].

Claim 15:

Kaufman discloses a machine-readable medium having stored thereon a set of instructions, which if executed by a machine cause the machine to perform a method comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "performing a plurality of iterations of an inner loop of an hash algorithm in parallel, the plurality of iterations performed in parallel being limited, at least in part, by dependencies between each of the plurality of iterations of the inner loop") [column 1 lines 20-31].
- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a

specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "adding initial values of a plurality of chaining variables to final values of the plurality of chaining variables, the final values being a result of performing the plurality of iterations of the inner loop") [column 9 lines 41-60].

Claim 16:

Kaufman discloses a machine-readable medium having stored thereon a set of instructions, which if executed by a machine cause the machine to perform a method as in Claim 15 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a

related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "the method further comprises controlling scheduling of operations performed as a result of performing the plurality of iterations of the inner loop, the scheduling being controlled so as to minimize a critical path among the operations") [column 1 lines 20-31].

Claim 17:

Kaufman discloses a machine-readable medium having stored thereon a set of instructions, which if executed by a machine cause the machine to perform a method as in Claim 16 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "the critical path depends upon the dependencies between the plurality of iterations of the inner loop") [column 1 lines 20-31].

Claim 18:

Kaufman discloses a machine-readable medium having stored thereon a set of instructions, which if executed by a machine cause the machine to perform a method as in Claim 17 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "decoding the inner loop of the hash algorithm into a first number of operational stages, the first number of operational stages being equal to at least the plurality of iterations") [column 9 lines 41-60].

Claim 19:

Kaufman discloses a machine-readable medium having stored thereon a set of instructions, which if executed by a machine cause the machine to perform a method as in Claim 18 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the inner loop is to be performed to process a first number of data elements transmitted over a network") [column 9 lines 41-60].

Claim 20:

Kaufman discloses a machine-readable medium having stored thereon a set of instructions, which if executed by a machine cause the machine to perform a method as in Claim 19 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the first number of operational stages is at least 83 and the first number of data elements comprises 512 bits") [column 9 lines 41-60].

Claim 21:

Kaufman discloses a method comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "performing a hash algorithm within a pipelined processor by performing a plurality of iterations of an inner loop of the hash algorithm in parallel; generating a plurality of output data elements as a result of performing the hash algorithm") [column 9 lines 41-60].

Claim 22:

Kaufman discloses a method as in Claim 21 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "scheduling operations associated with the plurality of iterations so as to facilitate a maximum number of the operations to be performed in parallel") [column 1 lines 20-31].

Claim 23:

Kaufman discloses a method as in Claim 22 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password

guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "the maximum number depends upon dependencies between the operations") [column 1 lines 20-31].

Claim 24:

Kaufman discloses a method as in Claim 22 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "the output data elements are transmitted within a computer network") [column 1 lines 20-31].

Claim 27:

Kaufman discloses a system comprising,

- "In accordance with the invention, each user 512, 514 is provided with a workstation 516, 518. Each workstation 516, 518 may be connected to a number of resources such as one or more disk storage mechanisms 504; communications equipment 506 such as modems (not shown); printers 508; secondary computers 510; and other equipment 511. For clarity of illustration, FIG. 5 only shows a limited number of interconnections and

components. Each user 512, 514 is also provided with a passive authentication token generator 520, 522 to assist the user 512, 514 in interacting with the authentication server 502. The token generators 520, 522 may, for example, comprise units such as SecurID.TM. units made by Security Dynamics, Inc of Cambridge, Mass. As described in greater detail below, the token generators 520, 522 may instead comprise active token generators, in accordance with an alternative embodiment of the invention" (i.e. "a memory unit to store operations of a hash algorithm") [column 8 lines 47-63].

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "a pipelined processor to perform the operations of the hash algorithm by performing iterations of an inner loop of the hash algorithm within separate pipeline stages of the pipelined processor") [column 1 lines 20-31].

Claim 28:

Kaufman discloses a system as in Claim 27 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified

system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "the operations are scheduled so as to minimize the number dependencies among the operations") [column 1 lines 20-31].

Claim 29:

Kaufman discloses a system as in Claim 28 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "a bus upon which to drive data generated by performing the hash algorithm within the pipelined processor") [column 1 lines 20-31].

Claim 30:

Kaufman discloses a system as in Claim 28 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "a bus to receive data to be operated on by the pipelined processor to perform the hash algorithm") [column 1 lines 20-31].

Claim 31:

Kaufman discloses a system as in Claim 30 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data

item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "512 bits of data is to be processed by at least 83 pipeline stages of the pipelined processor") [column 9 lines 41-60].

Claim 32:

Kaufman discloses a system as in Claim 27 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "the pipelined processor is a network processor coupled to a network") [column 1 lines 20-31].

Claim 33:

Kaufman discloses a system as in Claim 32 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "a host processor coupled to the network processor to perform a portion of the hash algorithm") [column 1 lines 20-31].

Claim 34:

Kaufman discloses a system as in Claim 27 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data

item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the hash algorithm is chosen from a group of secure hash algorithms (SHA) consisting of SHA-1, SHA-128, SHA-196, SHA-256, and message digest 5 (MD5)") [column 9 lines 41-60].

Claim 35:

Kaufman discloses an apparatus comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "execution means for performing iterations of an inner loop of a hash algorithm in parallel including") [column 1 lines 20-31].

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "first means for adding a first constant to a first data word to yield a first result; second means for adding the first result a first chaining variable, performing a first function on a second, third, and fourth chaining variable to yield a second result, and adding the first constant to a second data word to yield a third result; third means for adding the second result to the sum of a fifth chaining variable and the first result, adding the first constant to a third data word, adding the third result to the fourth chaining variable, performing the first function on the first, second, and third chaining variables after they each of have been shifted by a plurality of bits; adding means for adding an

initial state of the first, second, third, fourth, and fifth chaining variables to a final state of the first, second, third, fourth, and fifth chaining variables, respectively; scheduling means for scheduling operations associated with the hash algorithm") [column 9 lines 41-60].

Claim 36:

Kaufman discloses an apparatus as in Claim 35 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the execution means is a pipelined architecture and wherein each of the

first, second, and third means are pipeline stages of the pipelined architecture") [column 9 lines 41-60].

Claim 37:

Kaufman discloses an apparatus as in Claim 35 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the scheduling means is a controller to schedule operations associated with the inner loop according to dependencies among the operations") [column 9 lines 41-60].

Claim 38:

Kaufman discloses an apparatus as in Claim 36 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication tokens" (i.e. "each iteration of the inner loop requires three pipeline stages to perform the iteration") [column 1 lines 20-31].

Claim 39:

Kaufman discloses an apparatus as in Claim 38 above further comprising,

- "In one aspect, the invention pertains to a method by which a server in a distributed computing system may authenticate a user, authorizing access by the user to specified system resources and establishing a shared secret key with which to protect subsequent messages. In a specific embodiment, the invention pertains to a method by which an authentication server in a distributed computing system may transmit an authentication "ticket" to a user, authorizing access by the user to specified system resources. In a related aspect, the invention pertains to a method of increasing the difficulty of password guessing attacks in a distributed authentication scheme that employs authentication

tokens" (i.e. "the adding means comprises the same number of pipeline stages as chaining variables") [column 1 lines 20-31].

Claim 40:

Kaufman discloses an apparatus as in Claim 35 above further comprising,

- "In task 606, the workstation 516 computes a "transmission code" based upon the password and the token. The transmission code is calculated by using a first "hashing algorithm." As used herein, "hashing algorithm" is used to describe a one-way routine for transmuting multiple input data items, by concatenating selected items of the input data and performing a "hashing equation" upon one or more items of the input data, in a specified order. As used herein, "hashing equation," is understood to include any one-way routine for transmuting a single input data item of numeric, alphabetic, or alphanumeric characters into an output sequence of characters, wherein the input data item cannot be readily derived from the output sequence. Hashing equations are also understood to be consistent, in that each time a particular hashing equation is performed on a given input data item, the hashing equation produces the same output sequence. In an exemplary embodiment of the invention, the first hashing algorithm utilizes a hashing equation such as RSA Data Security's RSA MD2, RSA MD4, or RSA MD5, or the National Institute for Science and Technology proposal entitled "DHA" (Digital Hash Algorithm)" (i.e. "the hash algorithm is chosen from a group of secure hash algorithms (SHA) consisting of SHA-1, SHA-128, SHA-196, SHA-256, and message digest 5 (MD5)") [column 9 lines 41-60].

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 14, 25, 26, & 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaufman (US-5491752-A).

Claim 14:

Kaufman discloses an apparatus as in Claim 9 above, but does not disclose, "the network processor architecture is to perform the hash algorithm at an operating frequency of at least 1.4 GHz," However, Kaufman discloses that, "the invention pertains to a method by which a server in a distributed computing system," therefore it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include the feature in the applicant's invention in the invention as disclosed by Kaufman for the purposes of ensuring that the distributed computing system (i.e. pipelined) is scaled enabling it to handle simultaneous hash algorithm operations.

Claim 25:

Kaufman discloses a method as in Claim 21 above, but does not disclose, "the hash algorithm is performed at substantially the same frequency as the operating frequency of the processor." However, Kaufman does disclose that, "the invention pertains to a method by which a server in a distributed computing system," therefore it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include the feature in the applicant's

invention in the invention as disclosed by Kaufman for the purposes of ensuring that the distributed computing system (i.e. pipelined) is synchronize to handle simultaneous hash algorithm operations.

Claim 26:

Kaufman discloses a method as in Claim 21 above, but does not disclose, "the hash algorithm is performed at approximately 1.4 GHz." However, Kaufman discloses that, "the invention pertains to a method by which a server in a distributed computing system" [column 1 lines 20-21], therefore it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include the feature in the applicant's invention in the invention as disclosed by Kaufman for the purposes of ensuring that the distributed computing system (i.e. pipelined) is scaled enabling it to handle simultaneous hash algorithm operations.

Claim 41:

Kaufman discloses an apparatus as in Claim 35 above, but does not disclose, "the plurality of bits s 30." However, Kaufman does disclose, "the modified password is concatenated onto the token to form a concatenation, and this concatenation is modified by the hashing equation" [column 10 lines 10-12]. Therefore, it would have been obvious to one having ordinary skill in the art at the time of the applicant's invention to include the feature of the applicant's invention in the invention as disclosed by Kaufman for the purposes of accommodating for the assembling, hiding, and padding of data for encryption/decryption.

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

   a. Jones (US-6134603-A)

   b. Fielder (US-5963646-A)

   c. Hubbard (US-6847995-B1)

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Myhre, can be reached at 571-270-1065. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
01/16/2007

James Myhre
Supervisory Patent Examiner